КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (3), 2019
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2019.3.8896
УДК 004.62

Бржевська Зореслава Михайлівна
Аспірант, асистент кафедри Інформаційної та кібернетичної безпеки
Державний університет телекомунікацій, Київ, Україна
OrcID 0000-0002-7029-9525
zoreska.puzniak@gmail.com

Довженко Надія Михайлівна
Кандидат технічних наук, доцент кафедри Інформаційної та кібернетичної безпеки
Державний університет телекомунікацій, Київ, Україна
OrcID 0000-0003-4164-0066
nadezhdadovzhenko@gmail.com

Киричок Роман Васильович
Аспірант, асистент кафедри Інформаційної та кібернетичної безпеки
Державний університет телекомунікацій, Київ, Україна
OrcID 0000-0002-9919-9691
kyrychokr@gmail.com

Гайдур Галина Іванівна
Доктор технічних наук, доцент, завідуюча кафедри Інформаційної та кібернетичної безпеки
Державний університет телекомунікацій, Київ, Україна
OrcID 0000-0003-0591-3290
gaydurg@gmail.com

Аносов Андрій Олександрович
Кандидат військових наук, доцент, доцент кафедри Інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, Київ, Україна
OrcID 0000-0002-2973-6033
a.anosov@kubg.edu.ua

ІНФОРМАЦІЙНІ ВІЙНИ: ПРОБЛЕМИ, ЗАГРОЗИ ТА ПРОТИДІЯ

Анотація. У статті розглянуто проблеми вразливості Української держави в умовах інформаційної війни. Описано основні загрози, серед них: руйнування єдиного інформаційного простору держави; маніпуляція суспільною, недостатня координація діяльності органів державної влади, слабкість системи освіти та виховання, протиправне застосування спеціальних засобів впливу на суспільну свідомість, загострення міжнародної конкуренції за володіння інформаційними технологіями та ресурсами; діяльність міжнародних терористичних організацій; недостатність нормативної правової бази, що регулює відносини в інформаційній сфері, а також недостатня практика застосування права. В інформаційній війні виділяються три основних мети: контроль інформаційного простору і забезпечення захисту своєї інформації від ворожих дій; використання контролю над інформаційним простором для проведення інформаційних атак на противника; підвищення загальної ефективності збройних інформаційних функцій. Розглянуто складові інформаційних воєн та описано пріоритетні напрями державної інформаційної політики та важливі кроки з боку владних органів України. Формування суспільної свідомості за допомогою суб'єктів інформаційної війни з використанням методів психологічного впливу стає найбільш ефективним способом контролю і маніпуляції як всередині держави, так і за її межами. Все залежить від того, хто фактично визначає інформаційний контент. Таким чином, наше ставлення до проблем і явищ, навіть сам підхід до того, що вважати проблемою або явищем, багато в чому визначені тими, хто контролює світ комунікацій.

Ключові слова. інформаційна безпека України, національний інформаційний простір; інформаційні загрози; інформаційно-психологічні впливи; інформаційні війни та операції; інформаційні ресурси, механізми протидії інформаційним загрозам; державна інформаційна політика.

1. ВСТУП

У зв'язку з розвитком сучасних соціальних, національних і геополітичних процесів відзначається різке зростання чисельності й глибини конфліктів у міжнародних та внутрішньодержавних відносинах. Свідоме загострення конфліктних ситуацій за певних умов реалізується через негативні інформаційні впливи на суспільні процеси, зокрема з боку засобів масової інформації (ЗМІ). Їх характер має тенденцію переходу від відверто воєнного протистояння до застосування широкого спектра інформаційних впливів для досягнення дискредитації міжнародного і внутрішнього іміджу людини чи країни-противника. На жаль, Україна сьогодні опинилася якраз на межі загроз в інформаційному просторі й повинна бути спроможною на адекватні реакції для захисту від них.

Інформаційне середовище завжди впливало на психічний стан людей, стереотипи їхньої поведінки в суспільстві й особистому житті, на їхні морально-етичні норми, духовні цінності. Цей вплив став особливо значущим наприкінці XX сторіччя, коли інформаційно-комунікаційні процеси в суспільстві набагато активізувалась завдяки розвитку глобальних радіо- і телекомунікаційних систем, зокрема телебачення й Інтернету. Як наслідок, значно збільшилася ефективність маніпуляцій в інформаційних технологіях, які перетворилися в одне з основних джерел загроз інформаційно-психологічній безпеці особистості, окремих соціальних груп і суспільства в цілому. Інформаційно-психологічна безпека характеризує стан захищеності психіки людини від деструктивного інформаційного впливу та є складовою інформаційної безпеки [1].

Проблеми впливу інформаційних війн на суспільну свідомість досліджували: В. Богуш, О. Юдін, Я. Варивода, І. Воробйова, Б. Грушин, Д. Думанський, С. Кара-Мурза, М. Лібікі, В. Лисенко, А. Мануйло, Д. Ольшанський, Г. Почепцов, П. Шевчук та інші вчені.

2. ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Термін «інформаційна війна» став звичним як у засобах масової інформації, так і в лексиці політичних сил. Часто даний термін сприймається як «злив компромату», якому значною мірою сприяє засіб масової комунікації - Інтернет. Саме через Інтернет безконтрольно поширюються компрометуючі матеріали, «вкидається» у суспільство потрібна й своєчасна інформація, яку друковані і електронні ЗМІ тиражують, уже посилаючись на джерела в Інтернеті.

Розглянемо проблеми, що роблять Українську державу вразливою в інформаційній війні. По - перше, глобальні інформаційні мережі, що перебувають поза контролем, продовжують стрімко розвиватися. Буквально щодня з'являються нові електронні ресурси, серед яких засоби масової інформації, сайти різних радикальних угруповань та ін.

По - друге, вдосконалюються засоби і способи доставки інформаційно - пропагандистських матеріалів до аудиторії у ході інформаційно - психологічних операцій. У цих цілях усе більш активно використовуються такі нові медійні засоби, як

супутникове телебачення і радіо, цифрове телебачення, електронна пошта, засоби віртуальної реальності й ін.

По - третє, зростає кількість засобів спеціального програмно - математичного впливу на ресурси інформаційних систем, при цьому самі ці засоби з розвитком глобальних мереж стали широко доступні, що веде збільшення хакерських атак на інформаційні ресурси держави.

По - четверте, стає усе більше систем супутникового зв'язку, технічні характеристики яких усе більше вдосконалюються.

По - п'яте, розвиваються науково - дослідні програми щодо створення технічних засобів маніпулювання свідомістю.

По - шосте, недостатньо ефективною є підготовка випускників вищих навчальних закладів за спеціальностями, пов'язаними з інформаційними технологіями. Крім того, спостерігається їхній масовий виїзд за рубіж. У результаті цього Україна може залишитися без кваліфікованих фахівців, які займаються розробкою і впровадженням нових інформаційних технологій у систему інформаційної безпеки держави.

По - сьоме, низький рівень розвитку комунікацій. Практично відсутня культура використання ліцензійного програмного забезпечення. Фактично на дуже великій кількості ПК встановлені піратські операційні системи, зокрема Windows XP та Windows 7, технічна підтримка яких вже давно припинилася і вони більше не оновлюються, а значить не вирішуються вразливості в самій операційній системі, що дозволяє вірусам з легкістю самостійно потрапляти на комп’ютери і довго залишатись непомітними. Нездатність населення купувати дороге антивірусне ПЗ чи інші програми для інформаційного захисту призводить до того, що багато комп’ютерів виявляються не захищеними [2].

По статистиці антивірусної лабораторії Zillya! Близько 25-35% комп’ютерів в Україні заражені вірусами.

Основними загрозами відносно вищеперерахованих проблем можуть бути:

- Руйнування єдиного інформаційного простору держави;
- Блокування на неусвідомленому рівні свободи волевиявлення людини, прищеплювання їй синдрому залежності;
- Маніпуляція суспільною свідомістю з використанням засобів масової інформації та спеціальних засобів впливу.
- Недостатня координація діяльності органів державної влади та органів місцевого самоврядування з формування реалізації єдиної державної політики в галузі інформаційної безпеки;
- Слабкість системи освіти та виховання, недостатня кількість кваліфікованих кадрів у галузі інформаційної безпеки.
- Протиправне застосування спеціальних засобів впливу на індивідуальну, групову та суспільну свідомість;

ISSN 2663 - 4023

- Загострення міжнародної конкуренції за володіння інформаційними технологіями та ресурсами;
- Діяльність міжнародних терористичних організацій;
- Недостатність нормативної правової бази, що регулює відносини в інформаційній сфері, а також недостатня практика застосування права.

У кожній інформаційній війні є суб'єкт, тобто той чи ті, хто управляють інформаційними потоками. Безпосередньо до суб'єктів діяльності в інформаційному просторі суспільства, що реалізує державну інформаційну політику, відносяться:

1) органи державної влади та управління, які мають стабільні інтереси в інформаційному просторі; формують і контролюють національний інформаційний простір; створюють структурні підрозділи, у функції і завдання яких входить ведення інформаційної війни;

2) міжнародні організації, які мають стабільні інтереси в інформаційному просторі та беруть участь у формуванні інформаційного простору; використовують національні структури, інтегровані в міжнародні організації; створюють власний науково-технічний потенціал і використовують потенціал країн;

3) недержавні організації, які мають інтереси в інформаційному просторі; створюють власний сегмент інформаційного простору; створюють в рамках своїх структур підрозділи, у функції і завдання яких входить ведення інформаційного протиборства; створюють і використовують власний науково-технічний потенціал та використовують потенціал союзників, а також підтримуючих країни, які так чи інакше пов'язані з діяльністю цього суб'єкта; розробляють і закріплюють на рівні своєї офіційної ідеології певні цінності та ідеали

4) медіа-корпорації, основною функцією яких виступають поширення знань, ідей і цінностей, формування певних поглядів, уявлень і емоційних станів, людей і через них надання впливу на їх поведінку [3].

Формування суспільної свідомості за допомогою суб'єктів інформаційної війни з використанням методів психологічного впливу стає найбільш ефективним способом контролю і маніпуляції як всередині держави, так і за її межами. Все залежить від того, хто фактично визначає інформаційний контент. Таким чином, наше ставлення до проблем і явищ, навіть сам підхід до того, що вважати проблемою або явищем, багато в чому визначені тими, хто контролює світ комунікацій.

В інформаційній війні виділяються три основних мети: контроль інформаційного простору і забезпечення захисту своєї інформації від ворожих дій; використання контролю над інформаційним простором для проведення інформаційних атак на противника; підвищення загальної ефективності збройних інформаційних функцій. Можна виділити такі методи протидії інформаційним війнам та методи захисту інформаційного простору:

- пряме спростування;
- встановлення та знешкодження потенційних каналів просочування інформації;

- непряме спростування (наприклад, вказати на сумнівність джерела інформації; абсурдизація звинувачень; прив’язка джерела інформації до будь-якої негативної події; введення ще одного негативного факту, який легко піддається спростуванню);

- відвертання уваги. Варіантами можуть бути: відвертання ресурсів противника на інший об'єкт шляхом перенаправлення його на іншу діяльність (наприклад на відбиття інформаційної атаки на нього або на його протеже); введення в інформаційний простір нового сенсаційного повідомлення та відвертання уваги аудиторії на нову сенсацію; відвертання уваги аудиторії на малозначний факт у рамках поточної проблеми (концентрація уваги аудиторії на не принципових для вас моментах у рамках озвученої супротивником проблеми);

- мовчання у відповідь;

- мінімізація впливу (наприклад, акцентування на тому, що в повідомленні вказано на деякі правдиві події);

- дискредитація (умисні дії, спрямовані на підривання авторитету, іміджу і довіри до джерела негативної інформації). Варіантами можуть бути: обнародування компромату; обнародування віртуального компромату; негативна похвала (така дія має на увазі публічну похвалу об'єкту дискредитації, специфіка полягає в тому, як похвалили або хто похвалив, якщо похвала виходить від негативного у сприйнятті аудиторії об'єкту, то вона матиме також негативний характер); невмотивоване освистування (масове висловлювання негативного судження з приводу інформації або її джерела); громадське обурення (метод, близький до невмотивованого освистування, але зі зверненням до інших соціальних почуттів аудиторії);

- розмиття негативу (генерація нейтральної або позитивної інформації про об'єкт в об'ємах, що перевищують об'єми негативної інформації;

- доведення до абсурду (спосіб, що ґрунтується на виробленні імунітету у аудиторії до негативу про об'єкт).

В залежності від виду операції, що проводиться, інформаційна війна має відповідні складові, а саме: захист своїх соціальних та інформаційних систем від інформаційних засобів впливу противника; боротьба з державними системами управління противника різного призначення; війна в області політичної та економічної інформації; психологічна війна; комп’ютерна війна; кібернетична війна.

3. РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ

Як протидія масштабним інформаційним впливам, операціям та війнам, пріоритетними напрямами державної інформаційної політики та важливими кроками з боку владних органів України мають бути:

1) інтеграція України до світового та регіонального європейського інформаційного просторів;

2) інтеграція у міжнародні інформаційні та інформаційно-телекомунікаційні системи та організації;

3) створення власної національної моделі інформаційного простору та забезпечення розвитку інформаційного суспільства;

4) модернізації усієї системи інформаційної безпеки держави та формування й реалізація ефективної інформаційної політики;

5) удосконалення законодавства з питань інформаційної безпеки, узгодження національного законодавства з міжнародними стандартами та дієве правове регулювання інформаційних процесів;

6) розвиток національної інформаційної інфраструктури;

7) підвищення конкурентоспроможності вітчизняної інформаційної продукції та інформаційних послуг;

8) впровадження сучасних інформаційно-комунікативних технологій у процеси державного управління;

9) ефективна взаємодія органів державної влади та інститутів громадянського суспільства під час формування, реалізації та коригуванні державної політики в інформаційній сфері.

З метою недопущення інформаційної експансії, діяльність держави в інформаційному просторі має здійснюватись за такими напрямами:

1) реалізація упереджувальної стратегії та тактики (превентивні заходи);

2) здійснення реагувальної стратегії (оперативне реагування на інформаційні атаки супротивника та активний наступ);

3) захист національного інформаційного простору. Головна ціль – забезпечення домінування та медійної переваги в інформаційному просторі. Крім того, пріоритетними завданнями інформаційних структур владних органів мають бути: контроль за інформаційними потоками; надання об'єктивної, вичерпної інформації, представлення фахових коментарів та пояснень щодо подій; систематичне висвітлення офіційної позиції посадових осіб та політичних лідерів [4].

4. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Враховуючи надвисокий ступінь небезпеки, що несуть своєю діяльністю суб'єкти інформаційних війн усім державам (зокрема їх органам державної влади), державним структурам та міжнародним організаціям необхідно виробити відповідну нормативно-правову базу з урахуванням усіх можливостей сучасних інформаційно-телекомунікаційних технологій; звернути першочергову увагу на вироблення та розвиток інформаційно-телекомунікаційних технологій у сфері державного управління, підвищення здатності органів державної влади і місцевого самоврядування до використання ефективних технологій управління та організацію конструктивної взаємодії з громадськістю; звернути увагу на недостатній рівень підготовки кадрів в галузі створення та використання інформаційно-телекомунікаційних технологій та розробити низку заходів щодо підвищення зазначеного рівня.

Отже, в умовах сучасних інформаційних протистоянь, національний інформаційний простір України є недостатньо захищеним від негативних пропагандистських інформаційно-психологічних впливів, загроз. Тому створення потужної та ефективної системи інформаційної безпеки України, розроблення дієвих

стратегій і тактик протидії загрозам повинні стати пріоритетними завданнями органів державної влади та недержавних інститутів.

Перспективами подальших наукових досліджень є: аналіз зарубіжного досвіду протидії інформаційним впливам, а також глибше дослідження технологій здійснення інформаційних операцій та війн.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] В. Богуш, В. Кривуца та А. Кудін, Інформаційна безпека : Термінологічний навчальний довідник. Київ: ООО «Д.В.К.», 2004.

[2] О. Маруненко, "«Зовнішні і внутрішні інформаційні війни у медійному просторі України»", Український науковий журнал «Освіта регіону: політологія, психологія, комунікації», №4, стор. 91-95, 2011.

[3] В. Богуш та О. Юдін, Інформаційна безпека держави, 1st ed. Київ: МК-Прес, 2005.

[4] У. Ільницька, "«Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам»", Політичні науки, №. 1(2), стор. 27-32, 2016.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (3), 2019
ISSN 2663 - 4023

Zoreslava M. Brzhevska
Postgraduate student, assistant professor of information and cybersecurity department
State University of Telecommunications, Kyiv, Ukraine
OrcID 0000-0002-7029-9525
zoreska.puzniak@gmail.com

Nadiia M. Dovzhenko
Candidate of sciences, assistant professor of information and cybernetic security department
State University of Telecommunications, Kyiv, Ukraine
OrcID 0000-0003-4164-0066
nadezhdadovzhenko@gmail.com

Roman V. Kyrychok
Postgraduate student, assistant professor of information and cybersecurity department
State University of Telecommunications, Kyiv, Ukraine
OrcID 0000-0002-9919-9691
kyrychokr@gmail.com

Galyna I. Gaidur
Ph.D., Associate Professor, Head of the Department of Information information and cybersecurity
State University of Telecommunications, Kyiv, Ukraine
OrcID 0000-0003-0591-3290
gaydurg@gmail.com

Andriy O. Anosov
Candidate of sciences, associate professor, assistant professor of information and cybernetic security department
Kyiv Boris Grinchenko University, Kyiv, Ukraine
OrcID 0000-0002-2973-6033
a.anosov@kubg.edu.ua

INFORMATION WAR: PROBLEMS, THREATS AND ANTIDES

Abstract. This article is about the problems of vulnerability of the Ukrainian state in the conditions of information warfare. The main threats are described, among them: the destruction of a single information space of the state; manipulation of the public, lack of coordination of state authorities, weakness of education and education, illegal use of special means of influence on public consciousness, aggravation of international competition for ownership of information technologies and resources; activities of international terrorist organizations; insufficiency of regulatory legal framework regulating relations in the information sphere, as well as insufficient application of law. In the information warfare, there are three main goals: control of the information space and the protection of their information from hostile acts; use of control over the information space for carrying out informational attacks on the enemy; increasing the overall effectiveness of armed information functions. The components of information wars are considered and the priority directions of the state information policy and important steps from the authorities of Ukraine are described. Formation of public consciousness with the help of subjects of information warfare using methods of psychological influence becomes the most effective way of control and manipulation, both within the state and beyond its borders. It all depends on who actually determines the content. Thus, our attitude to problems and phenomena, even the very approach to what is considered a problem or phenomenon, is largely determined by those who control the world of communications.

ISSN 2663 - 4023

Keywords. information security of Ukraine, national information space; information threats; informational and psychological influences; information wars and operations; information resources, mechanisms of counteraction to information threats; state information policy.

REFERENCES

[1] V. Bohush, V. Kryvutsa and A. Kudin, Informatsiyna bezpeka : Terminolohichnyy navchal′nyy dovidnyk. Kyiv: OOO «D.V.K.», 2004. (In Ukrainian)

[2] O. Marunenko, "«Zovnishni i vnutrishni informatsiyni viyny u mediynomu prostori Ukrayiny»", Ukrayins′kyy naukovyy zhurnal «Osvita rehionu: politolohiya, psykholohiya, komunikatsiyi», № 4, pp. 91-95, 2011. (In Ukrainian)

[3] V. Bohush and O. Yudin, Informatsiyna bezpeka derzhavy, 1st ed. Kyiv: MK-Pres, 2005. (In Ukrainian)

[4] U. Il′nyts′ka, "«Informatsiyna bezpeka Ukrayiny: suchasni vyklyky, zahrozy ta mekhanizmy protydiyi nehatyvnym informatsiyno-psykholohichnym vplyvam»", Politychni nauky, № 1(2), pp. 27-32, 2016. [Accessed 26 March 2019]. (In Ukrainian)